CLAIMS

1. A method of transmission and reception of a scrambled data stream in which the scrambled data stream is transmitted to a decoder and thereafter passed to and descrambled by a portable security module inserted in the decoder and characterised in that the data stream is passed from the security module to the decoder in an encrypted form, to be decrypted and subsequently used by the decoder.

2. A method as claimed in claim 1, in which the data stream is encrypted in the security module by a first encryption key before being passed back to the decoder for decryption using an equivalent of the first key.

3. A method as claimed in claim 2 in which the data stream is encrypted in the security module by a first encryption key variable in dependence on a decoder identity value, the decoder possessing an equivalent of the key and value necessary to decrypt the data stream.

4. A method as claimed in claim 3 in which the decoder identity value is encrypted by a personalised key known to the security module and transmitter, the decoder identity value being transmitted in an encrypted form to the ~~decoder~~ security module for communication to the security module.

5. A method as claimed in 3 in which the decoder identity value is encrypted by a personalised key known to the security module, the encrypted decoder identity value being stored in the decoder during manufacture for communication to the security module upon insertion of the security module in the decoder.

6. A method as claimed in claim 2 in which the data stream is encrypted in the security module by a first encryption key dependant on a random or pseudo-random number.

7. A method as claimed in claim 6, in which the random number is communicated between the decoder and security module encrypted by a second encryption key.

8. A method as claimed in claim 7, in which the random number is generated and encrypted by the second encryption key in the security module and communicated to the decoder for decryption by an equivalent of the second key stored in the decoder.

9. A method as claimed in claim 7 in which the random number is generated and encrypted by the second encryption key at the decoder and communicated to the security module for decryption by an equivalent of the second key stored in the security module.

10. A method as claimed in claim 9 in which the second key used to encrypt the random number in the decoder corresponds to a public key, the security module being provided with the equivalent private key necessary to decrypt the random number value.

11. A method as claimed in claim 9 ~~or 10~~ in which at least the second key held by the security module is unique to that security module.

12. A method as claimed in ~~any of claims 7 to 11~~ 7, in which the second key held by the decoder is encrypted by a third key before communication to the decoder, the decoder possessing the corresponding third key so as to hereby decrypt and verify the second decoder key.

13. A method as claimed in claim 12, in which the third key used to encrypt the second decoder key is a private key, the decoder possessing the equivalent public key to decrypt and verify the communicated second key.

14. A method as claimed in claim ~~1~~ 11 in which the data stream is encrypted at the point of transmission by a first encryption key and decrypted by the decoder by an equivalent of this key.

15. A method as claimed in claim 14 in which the data stream is encrypted at the point of transmission by a first encryption key dependant on a variable known to both the transmitter and the decoder and decrypted at the decoder by an equivalent of this key and variable.

16. A method as claimed in claim 15 in which the variable corresponds to the real time and/or date of transmission.

17. A method as claimed in ~~any of claims 14 to 16~~ 14 in which the first encrypted data stream is further scrambled at the point of transmission, descrambled in the security module and then passed in its first encrypted form to the decoder.

18. A method of transmission and reception of scrambled data combining a method of encryption of the data stream in the card as claimed in any of claims 2 to 13, separately or in combination, together with a method of encryption of the control word at the point of transmission, as claimed in any of claims 14 to 17.

19. A method as claimed in ~~any of claims 1 to 18~~ 24 in which the data stream passed in encrypted form between the security module and decoder comprises audiovisual data.

20. A method as claimed in ~~any of claims 1 to 18~~ 24 in which the data stream passed in encrypted form between the security module and decoder comprises a control word stream, the control word stream once decrypted by the decoder being thereafter used by the decoder to descramble associate scrambled audiovisual data.

21. A method as claimed in ~~any preceding claim~~ 24 in which the scrambled data stream is transmitted as part of a television broadcast.

22. A decoder and portable security module adapted for use in a method as claimed in any preceding claim.

23. A method of transmission and reception of a scrambled data stream substantially as herein described.